

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-297541

(43)Date of publication of application : 11.10.2002

(51)Int.Cl.

G06F 15/00

G09C 1/00

(21)Application number : 2001-102393

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 30.03.2001

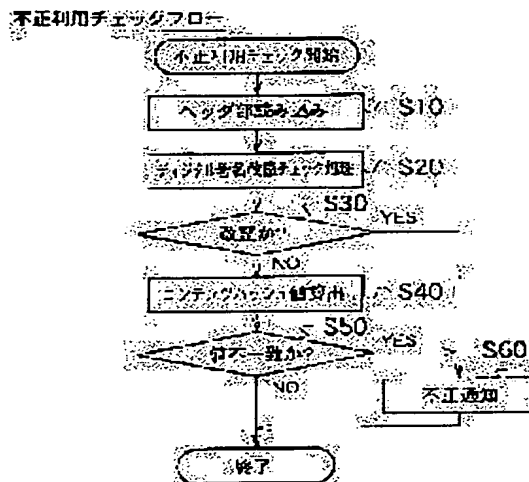
(72)Inventor : KUROKAWA KIYOSHI
AZUMA SHOZO
SANO MUTSUO

(54) UNAUTHORIZED UTILIZATION NOTICE METHOD, ITS DEVICE AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an unauthorized utilization notice method, its device and program capable of monitoring unauthorized utilization for contents downloaded freely at a client-side without making a user be conscious.

SOLUTION: This method comprises: reading a hash value of contents described before the circulation from a contents ID attached to the contents after circulation (S10); calculating a hash value of contents for the contents after the circulation by using the same hash function as the hash function used in calculation of the hash value of contents described before the circulation (S40); determining whether the unauthorized utilization is present depending on whether the hash value of contents before-and-after the circulation are matched with each other (S50); and sending the unauthorized utilization information indicating the unauthorized utilization in an address of a management server included in contents ID when the unauthorized utilization is present (step S60).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

BEST AVAILABLE COPY

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2 0 0 2 - 2 9 7 5 4 1

(P 2 0 0 2 - 2 9 7 5 4 1 A)

(43) 公開日 平成14年10月11日 (2002. 10. 11)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5B085
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 A 5J104
			6 4 0 D

審査請求 未請求 請求項の数 3

O L

(全 8 頁)

(21) 出願番号 特願2001-102393 (P2001-102393)

(22) 出願日 平成13年3月30日 (2001. 3. 30)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 黒川 清

東京都千代田区大手町二丁目3番1号 日本
電信電話株式会社内

(72) 発明者 東 正造

東京都千代田区大手町二丁目3番1号 日本
電信電話株式会社内

(74) 代理人 100083806

弁理士 三好 秀和 (外1名)

最終頁に続く

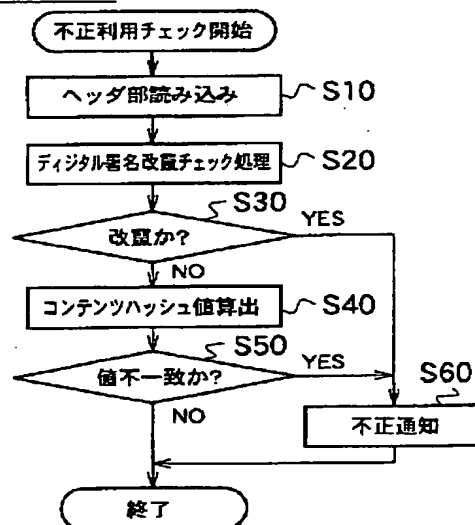
(54) 【発明の名称】 不正利用通知方法、不正利用通知装置および不正利用通知プログラム

(57) 【要約】

【課題】 本発明は、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知プログラムを提供することにある。

【解決手段】 流通後のコンテンツに添付されているコンテンツ ID から流通前に記述されたコンテンツハッシュ値を読み出し (S 1 0)、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出 (S 4 0) しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断 (S 5 0) し、不正利用があった場合には、コンテンツ ID に含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信 (ステップ S 6 0) する。

不正利用チェックフロー



【特許請求の範囲】

【請求項 1】 配信されたコンテンツの流過程での不正利用を検出して通知する不正利用通知方法であって、流通後のコンテンツに添付されているコンテンツ ID から流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、

流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、

流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、

不正利用があった場合には、コンテンツ ID に含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知方法。

【請求項 2】 配信されたコンテンツの流過程での不正利用を検出して通知する不正利用通知装置であって、流通後のコンテンツに添付されているコンテンツ ID から流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、

流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、

流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、

不正利用があった場合には、コンテンツ ID に含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを特徴とする不正利用通知装置。

【請求項 3】 配信されたコンテンツの流過程での不正利用を検出して通知する不正利用通知プログラムであって、

流通後のコンテンツに添付されているコンテンツ ID から流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、

流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、

流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、

不正利用があった場合には、コンテンツ ID に含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知プログラム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、広範に流通するコンテンツの流通監視を行い、不正利用を検出して不正利用情報を通知する不正利用通知方法および不正利用通知装置に関する。

【0002】

【従来の技術】従来の不正利用通知方法としては、電子透かし技術を用いてコンテンツを一意に識別できるコンテンツ ID などを予めコンテンツに埋め込んでおいて流通させ、不正利用検出システムにより、正規配布先の URL と埋め込んだコンテンツ ID との対応関係をチェックして不正利用を監視するというネットボリス技術が知られている。

【0003】このような不正利用検出システムにおいて用いられている検出技術としては、以下の技術が知られている。

【0004】(1) 透かし読み取り機能を有する探索ロボットにより、Web サイトのページに含まれているコンテンツをトップダウン的に探索する技術。

【0005】(2) 特定ネットワークに設けられた特定ノードのゲートウェーやサーバに透かし読み取りフィルタを組み込んでおき、このフィルタを通過するコンテンツを全てチェックする技術。

【0006】(3) 利用者のブラウザのダウンロードモジュールに透かし読み取りツールを予めプラグインしておき、Web サーバからダウンロードしたコンテンツのコンテンツ ID とアクセスサイトの URL をコンテンツ ID 管理センタに通知してチェックする、ボトムアップ的な利用者協力型がある。

【0007】例えば、エム研 (<http://www.mken.co.jp/>) では、以下のようなサービスを行っている。

【0008】このサービスでは、透かし検知ロボットにより、透かし入りコンテンツに関連しそうな単語をキーワードとしてサーチエンジンでピックアップした Web サイトを中心に回るイエローリスト巡回方式と、著作権違反の可能性のあるコンテンツを持っている Web サイトを中心に回るグレーリスト巡回方式とに従って 24 時間常時インターネットを監視しており、世界中のホームページを巡回して例えば、「acuaporta」の電子透かしを埋め込んだコンテンツをデコードして監視し、不正にコピー、改竄されてネットワーク上に掲示されたコンテンツの発見に努めている。

【0009】

【発明が解決しようとする課題】このように、従来の不正利用通知方法では、著作権保護技術によりカプセル化を行い、専用のソフトを利用して、鍵・利用条件・クライアント情報などの認証を行うことにより不正利用を防止していた。また、管理サーバに不正利用の疑いのあるコンテンツを転送し、コンテンツに予め埋め込んである

電子透かしなどを検出していた。

【0010】しかしながら、従来の不正利用通知方法にあっては、管理サーバに不正利用の疑いのあるコンテンツを持ち込む必要があるため、インターネットの普及に伴って管理サーバの稼働負荷が増大するとともに、管理サーバの増設が必要になるといった問題があった。

【0011】そこで、管理サーバの稼働負荷の増大や管理サーバの増設などを行わずに、コンテンツを再生するクライアント側のメディアプレイヤーに不正利用を検出して通知する方法が求められてきた。

【0012】本発明は、上記に鑑みてなされたもので、その目的としては、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知装置を提供することにある。

【0013】

【課題を解決するための手段】請求項1記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知方法であって、流通後のコンテンツに添付されているコンテンツIDから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【0014】請求項2記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知装置であって、流通後のコンテンツに添付されているコンテンツIDから流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、不正利用があった場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを要旨とする。

【0015】請求項3記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知プログラムであって、流通後のコンテンツに添付されているコンテンツIDから

ら流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【0016】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【0017】図1は、本発明の一実施の形態に係る不正利用通知方法を適用可能なDRM処理フローの構成を示す図である。

【0018】図1に示すように、本システムには、コンテンツを作成するためのエンコーダ装置13、コンテンツを管理するためのDRM (Digital Rights Management) 装置17、コンテンツを配信するためのメディアサーバ21、コンテンツを再生するためのメディアプレイヤー23が設けられている。

【0019】エンコーダ装置13は、一般に符号器と呼ばれ、カメラからのライブ画像、マルチメディアファイル、クライアント（パーソナルコンピュータ）の画面情報などのメディアファイルA11を入力して一定の規則に従って符号化して指定形式の圧縮されたファイルに変換する機能を有しており、変換されたメディアファイルB15が出力される。

【0020】DRM装置17は、Webサーバからなり、Webサイトのメニューページや、情報の要求または支払いが行われる登録ページを提供して、登録ページ上から解凍のためのライセンスキーなどを与える機能を有している。特に、DRM装置17は、コンテンツを保護するためのライセンス管理や著作権管理機能によりコンテンツ管理を行っており、エンコーダ装置13により変換されたメディアファイルB15を入力して鍵番号とライセンスを取得するためのURL情報を付加し、メディアファイルB15に対して、エンコーダ装置13による変換の逆変換を行うことが可能な鍵番号とライセンス取得URL情報を用いて暗号化して一体のデータになるようにカプセル化し、このカプセル化されたメディアファイルC19をメディアサーバ21に送信する。なお、カプセル化されたメディアファイル19は、ライセンスとともに暗号化され「鍵」を用いなければ上述した逆変換が不可能なように保護されている。この「鍵」は、DRM装置17からメディアプレイヤー23に別途配布される。

【0021】また、カプセル化されたメディアファイル

10

20

30

40

50

19を利用者にダウンロードさせるためにサーバ上のWebサイトに置いたり、ストリーミングのためにメディアサーバ21上に置いたり、CD-ROMを媒体として配布したりする。

【0022】メディアプレイヤー23は、DRM装置17との通信機能をサポートしており、例えば、メディアサーバ21からカプセル化されたメディアファイルC19をダウンロードし、メディアファイルC19から抽出した鍵番号とコンテンツIDを抽出してDRM装置17に送信し、DRM装置17からこの鍵番号とコンテンツIDに対応する鍵と利用条件およびクライアント情報などの証明書が返信され、カプセル化されたメディアファイルC19がメディアファイル25に逆変換され、ライセンスに含まれている利用条件に従ってメディアファイル25がデコード機能により再生される。なお、ライセンスには、開始時刻、日付、期間、再生回数などのさまざまな権利行使するための利用条件を与えることができる。

【0023】また、保護されたメディアファイルC19を再生するためには、利用者はまずメディアファイルC19をメディアファイルB15に逆変換するためのライセンスキーを取得する必要がある。ライセンスキーの取得タイミングは、利用者が保護されたメディアコンテンツC19を取得しようと試みたときや、メディアファイルを初めて再生したときに自動的に開始される。

【0024】このときDRM装置17は、Webサイトのメニューページから情報の要求または支払いが行われるWebサイト上の登録ページに利用者を誘導し、利用者は誘導された登録ページ上から解凍のためのライセンスキーを取得することとなる。

【0025】また、メディアプレイヤー23は、メディアファイルC19を再生中に、このメディアプレイヤー23が存在するクライアント（パーソナルコンピュータ）上のコンテンツIDに準拠したメディアファイルを順次参照して、後述する不正利用チェックフローによりのメディアファイルの不正利用があるかどうかを確認する。

【0026】次に、図2は、コンテンツIDの詳細な構成に示す説明図である。

【0027】詳しくは、図2に示すように、コンテンツIDには、コンテンツに関する属性情報を特定するためにコンテンツに一意的に付与される識別子として、左側から、コンテンツに一意に付与される番号（ユニークコード）を表すIDセンタ管理番号、コンテンツのクリエイターや内容や種別や分類などに関する情報を表すコンテンツ属性、コンテンツの権利関係を表記する権利属性、権利の許諾・選任・確認に関する情報を表す権利運用属性、コンテンツの流通（＝売買）の履歴情報を表す流通属性、売買収益の分配に関する情報を表す分配属性、ID管理センタに任される自由領域を表す自由領域、デジタル署名やコンテンツハッシュ値などを表すシステム

領域などが設定されている。

【0028】さらに、コンテンツIDの構成要素には、コンテンツを特定するための情報と流通に関する情報、電子透かしの方式などシステムに関する情報がある。これらの表現方法には、ユニークコード、流通記述子（DCD：Distributed ContentDescription）があり、必要に応じて使い分ける。なお、流通記述子（DCD）は、コンテンツIDの中で権利者により予め規定された利用条件などの重要情報である。

10 【0029】このうち、システム領域には、図3に示すように、コンテンツとコンテンツID（流通記述子：DCD）をバンドルするためのデジタル署名とコンテンツハッシュ値が含まれており、これらを利用して不正チェックを行う。さらに、システム領域には、コンテンツデータと連結するためのコンテンツへのリンク、電子透かし情報、署名アルゴリズム情報、チェックディジットなどがある。

【0030】ここで、デジタル署名とコンテンツハッシュ値のデータ構造や数理的特徴を説明し、不正チェックをどのように行うかを説明する。

20 【0031】図3に示すように、公開鍵暗号方式に基づいたデジタル署名においては、署名作成者がその通信内容となるコンテンツ（電子文書）を署名者固有の署名鍵（秘密鍵）により暗号化し、署名付きコンテンツ（電子文書）の受信者がその署名鍵に対応する署名作成者の検証鍵（公開鍵）によりそのデジタル署名が本当に送信者の署名であるのかどうかを検証することができるという仕組みになっている。

30 【0032】従って、デジタル署名は、通信内容を暗号化したものを署名とするという技術的な特性から、署名そのものと通信内容である電子文書自体との結合性が強く、もし通信内容が通信途上で改竄されれば、後述する署名の検証過程によって、改竄されたという事実も検証することができるという利点がある。

【0033】具体的な実現方法の1つであるクリアデジタル署名（分離署名）は、図3に示すように、コンテンツデータとデジタル署名が分離されており、コンテンツデータはそのまま読み、一方、デジタル署名が記述されているシステム領域には、コンテンツ本文のコンテンツハッシュ値（秘密の計算式で計算した値）を含んでいる。

【0034】このため、デジタル署名が改竄された場合には、デジタル署名の署名対象となるコンテンツハッシュ値も同時に改竄されることになる。その結果、実際のコンテンツハッシュ値を計算して、計算されたコンテンツハッシュ値とコンテンツID中のコンテンツハッシュ値が異なり、デジタル署名の改竄を検出することができる。

50 【0035】ここで、図3に示すコンテンツハッシュ値は、予め決められたハッシュ関数により得られた値であ

り、ハッシュ関数には、不可逆な一方関数を含むため、コンテンツハッシュ値からコンテンツデータを再現することはできず、また同じコンテンツハッシュ値を持つ異なるコンテンツデータを作成することは極めて困難である。なお、ハッシュ関数としては、例えば、MD5、SHA1などが広く知られている。

【0036】また、具体的な検出過程では、このハッシュ関数は、与えられたコンテンツデータから固定長の疑似乱数を生成する演算手法であり、通信などの流通過程を通じてコンテンツデータを提供する際に、流通前のコンテンツデータからハッシュ関数を用いて求めておいたコンテンツハッシュ値をコンテンツIDのシステム領域から抽出しておき、流通後のコンテンツデータからハッシュ関数を用いて求めたコンテンツハッシュ値と比較すれば、コンテンツデータが通信などの流通途中で改竄されているかどうかを調べることができる。

【0037】次に、図4は、コンテンツの作成時におけるコンテンツIDの埋め込みフローである。

【0038】図4に示すように、メディアファイルA11として、音声ファイルに関してWAV、WMA、MP3などの識別子があり、映像ファイルに関してWMV、ASF、AVI、MPEG1などの識別子があり、その他のファイルの識別子としてBMPがある。メディアファイルA11は、二階層電子透かしをオプションとして扱うことができる。

【0039】エンコーダ装置13で変換されたメディアファイルB15として、WMA、WMV、ASFなどの識別子があり、これらのカプセル化されたメディアファイルB15のヘッダ情報へ上述したDCDを埋め込む。

【0040】DRM装置17でカプセル化されたメディアファイルC19は、上述したDCDをバインドする。

【0041】なお、メディアファイルA11は、IDセンタ管理番号からなるユニークコードを用いた二階層電子透かしをオプションとして扱うことができる。

【0042】ここで、二種類の異なる電子透かしを順次埋め込む二階層電子透かしについて説明する。

【0043】電子透かしには、多数の方式があり、すべての電子透かしを順次試みるとなると、検出時間が膨大になってしまう恐れがあるため、メタ電子透かしを用いて実電子透かしの種別情報を埋め込むようにする。この実電子透かしは、IDセンタの管理番号を埋め込むものであり、メタ電子透かしは、実透かしの種別情報を埋め込むものである。

【0044】検出手順は、メタ電子透かしの検出により実電子透かしの種別を特定し、さらに、特定した実透かしを検出するようにするので、二種類の異なる電子透かしにより埋め込まれたユニークコードの検出過程を複雑化でき、不正利用者による容易な解読をできないようにすることができる。

【0045】なお、ユニークコードは、IDセンタ管理

番号を示しており、その構成は以下の通りである。

【0046】(1) 地域コード (4bit)

世界を16地域に分割してセンタの番号付与が可能である。

【0047】(2) センタ番号 (8bit)

Registration Authority が発行し、IDセンタを識別する固定長の番号である。

【0048】(3) センタ内番号 (任意)

IDセンタが管理するコンテンツを識別する番号であり、IDセンタが任意に割付ける。

【0049】(4) バージョン番号 (4bit)

コンテンツIDのバージョンを2進数によるバイナリ表現を用いて規定した番号である。

【0050】次に、図5は、メディアプレイヤ23の機能構成を示す図である。

【0051】メディアプレイヤ23は、メディアファイル25の再生中に、メディアプレイヤ23が存在するクライアント上のコンテンツIDに準拠したファイルを順次チェックし、不正利用のメディアファイルを確認する。

【0052】図5に、メディアプレイヤ23の機能構成の一例を示す。メディアプレイヤ23は、認証部41、流通情報蓄積部43、不正利用チェック部45、メディア再生部47から構成されている。

【0053】また、メディアプレイヤ23により再生されるメディアファイルは、先頭からヘッダ情報、システム化領域、ディジタル署名、コンテンツハッシュ値、コンテンツ領域を有している。

【0054】認証部41は、入力されたメディアファイルから鍵番号とコンテンツIDを抽出してDRM装置17に送信し、DRM装置17から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。

【0055】流通情報蓄積部43は、過去に再生したメディアファイルのコンテンツIDから収集した流通属性を流通情報として蓄積する。

【0056】不正利用チェック部45は、クライアント上のメディアファイルをサーチし不正利用を検出するモジュールであり、その詳細な動作を図6に示す不正利用チェックフローにより処理される。

【0057】メディア再生部47は、DRM装置17から受信した利用条件に従ってメディアファイル25をデコード機能により再生する。このデコード機能は、エンコーダ装置13による符号化とは逆に、符号化されたメディアファイル25をメディアファイルA11に復号する機能である。

【0058】ここで、図5に示すメディアプレイヤ23での基本的な動作を説明する。

【0059】なお、パーソナルコンピュータからなるクライアントには、制御部にOSプログラムや制御データやアプリケーションプログラムを一時的に記憶するRA

10

20

30

40

50

Mと、制御プログラムやアプリケーションプログラムに従ってシステムを制御するCPUとが設けられている。また、ハードディスクHDに記録されているアプリケーションプログラムは、例えばパーソナルコンピュータに設けられたCD-ROMドライブなどを用いてCD-ROMなどの記録媒体からインストールされたプログラムであり、本発明の不正利用通知プログラムを記録した記録媒体などである。

【0060】クライアント上でメディアプレイヤー23の画面からメディアサーバ21のURLを指定してホームページを開き、メディアファイルを受信する。そして、認証部41では、入力されたメディアファイルから鍵番号とコンテンツIDを抽出してDRM装置17に送信する。そして、認証部41が、DRM装置17から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。そして、メディア再生部47では、メディアファイル25をDRM装置17から受信した開始時刻、日付、期間、再生回数などの利用条件に従ってメディアファイルA11に復号して再生する。

【0061】このメディア再生部47でメディアファイルの再生を行っている際に、並行して不正利用チェック部45は、バックグラウンドでクライアント上にある他のメディアファイルを対象にした不正利用チェックを行う。

【0062】図6において、不正利用チェックを開始すると、ステップS10では、メディアファイル25のコンテンツIDからヘッダ情報を読み込み、特に、流通後のメディアファイルに添付されているコンテンツIDから流通前に記述されたコンテンツハッシュ値とデジタル署名を読み出す。

【0063】そして、ステップS20では、デジタル署名の改竄チェック処理を行う。

【0064】すなわち、流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を計算して、計算された流通後のコンテンツハッシュ値とコンテンツID中に記述されている流通前のコンテンツハッシュ値が異なった場合には、デジタル署名の改竄があったこととなる。

【0065】そして、ステップS30では、改竄があるかどうかを判断する。改竄がない場合には、ステップS40に進み、流通後のコンテンツに対して流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を算出する。

【0066】そして、ステップS50では、算出した流通後のコンテンツハッシュ値がメディアファイル25のコンテンツIDから読み出した流通前のコンテンツハッシュ値と不一致かどうか判断する。

【0067】ここで、算出した流通後のコンテンツハッ

シュ値がメディアファイル25の流通前のコンテンツハッシュ値と一致した場合には、正常な利用であることを示しているのを、そのまま処理を終了する。

【0068】一方、ステップS30で改竄があると判断した場合、または、ステップS50で流通前後のコンテンツハッシュ値同士が不一致の場合、ステップS60に進み、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信し、処理を終了する。

【0069】このように、不正利用チェック部45において、メディアファイル25のデジタル署名とコンテンツハッシュ値の確認を行うので、当該メディアファイル25が不正利用かどうかを検出することができ、当該メディアファイル25が不正利用の場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することができる。

【0070】また、コンテンツIDに示されるセンタアドレス（センタサーバのURL）に、不正利用があったことを示す不正利用情報を通知することができる。なお、この不正利用情報には、コンテンツIDと存在場所（端末のIPアドレス）、不正利用チェック結果を含むこととする。

【0071】この結果、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができ、特に、メディアプレイヤーに適用することができる。また、クライアント側の不正監視手段として適用することができる。

【0072】また、メディアプレイヤーのバージョンアップに合わせて、新しいデジタル署名方式や新規チェック項目を追加した場合でも、不正利用検出フローを容易に改定することができる。

【0073】本実施の形態における効果は、流通後のコンテンツに添付されているコンテンツIDから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【0074】

【発明の効果】請求項1乃至3記載の本発明によれば、流通後のコンテンツに添付されているコンテンツIDから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と

10

20

30

40

50

同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツIDに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る不正利用通知方法を適用可能なDRM処理フローの構成を示す図である。

【図2】コンテンツIDの詳細な構成に示す説明図である。

【図3】DCDの詳細な構成に示す説明図である。

【図4】コンテンツ作成時のコンテンツIDの埋め込みフローである。

【図5】メディアプレイヤー23の機能構成を示す図である。

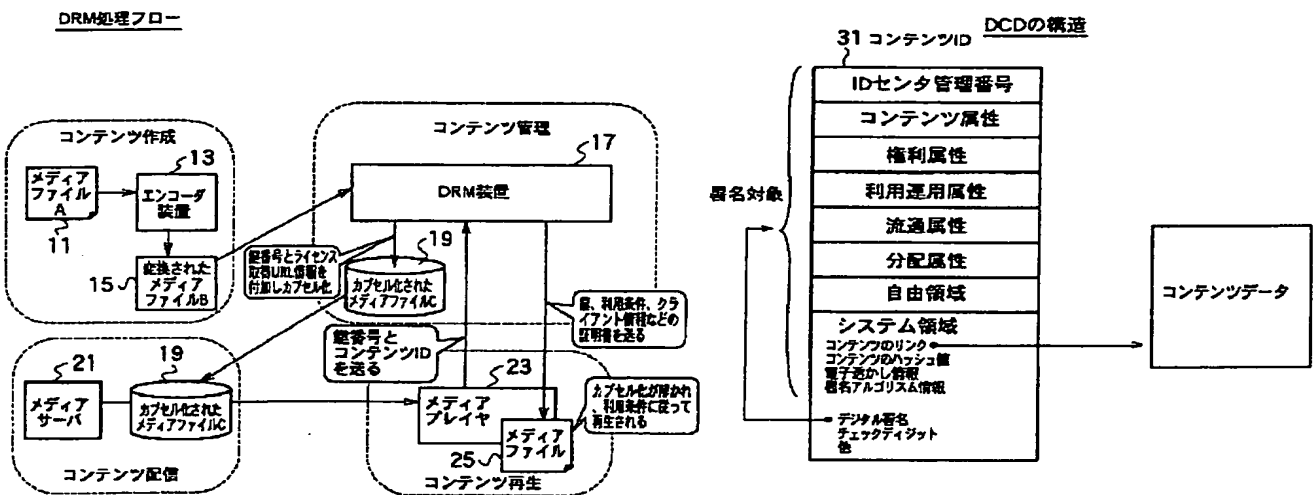
【図6】不正利用チェック部45の詳細な動作を説明するためのフローである。

【符号の説明】

- 13 エンコーダ装置
- 17 DRM装置17
- 21 メディアサーバ
- 23 メディアプレイヤー
- 25 メディアファイル
- 31 コンテンツID
- 41 認証部
- 43 流通情報蓄積部
- 45 不正利用チェック部
- 47 メディア再生部

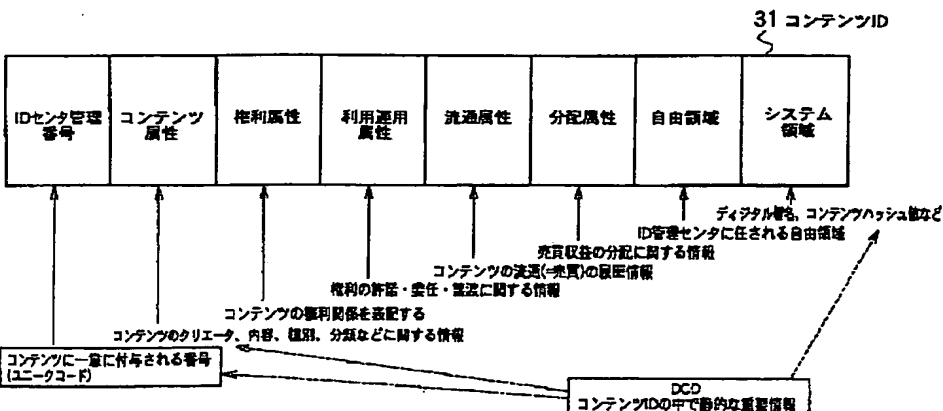
【図1】

【図3】



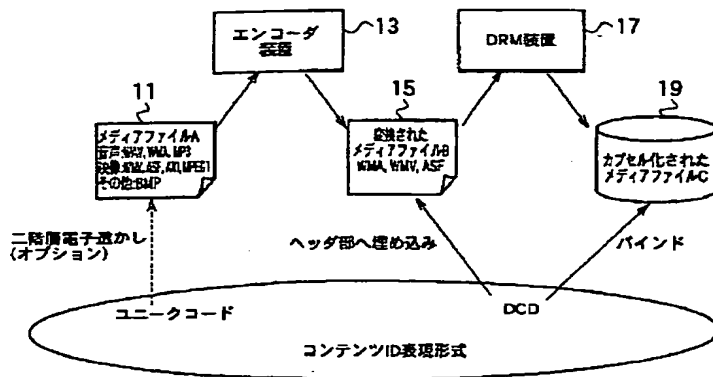
【図2】

コンテンツID (メディアプレイヤー→DRM部)



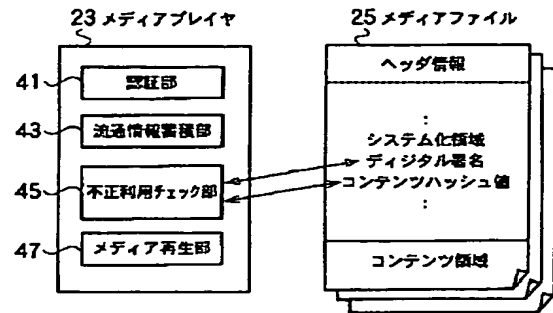
【図4】

コンテンツID埋め込みフロー



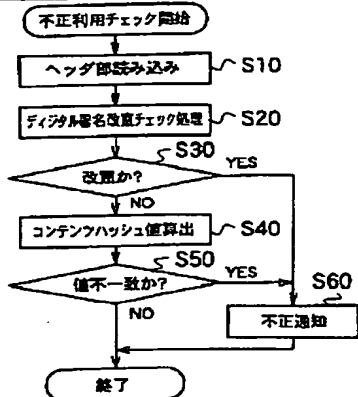
【図5】

プレイヤーの機能構成



【図6】

不正利用チェックフロー



フロントページの続き

(72)発明者 佐野 睦夫
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

Fターム(参考) 5B085 AE00
5J104 AA08 AA13 LA02 LA05 NA12
PA14

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.